

The invention claimed:

1. A computer-implemented method for determining network security threat level,
comprising the steps of:

5 receiving event data in response to identified network event detected by a
sensor;

 based upon the event data, perform the following step:

 determining a source threat value, the source threat value based upon a
source threat weight for a source IP address and a first range of IP network
10 addresses of which the source IP address is a member;

 determining a destination vulnerability value, the destination
vulnerability value based upon the network event in conjunction with a
destination IP address, a destination threat weight for the destination IP address,
and a threat level value associated with a second range of network IP address of
15 which the destination IP address is a member;

 determining an event validity value based upon the source IP address
and an event type

 determining event severity value based upon the event type;

 calculating an event threat level value based upon the source
threat value, the destination vulnerability value, the event validity value, and the
20 event severity value;

 calculating a host threat level value based upon a summation of
event threat level values for a host over a first time period associated with a
number of correlated events for the host in the first time period; and

25 calculating a differential threat level by associating the host
threat level value with a second host threat level value based upon a second time
period wherein the second time period exceeds the first time period.

2. The method of claim 1, further comprising the steps of:

30 comparing the event threat level value to an event alert value; and

generating an alarm when the event threat level value exceeds the event alert value.

3. The method of claim 1, further comprising the steps of:
comparing the compound host threat level value to a host alert value; and
5 generating an alarm when the host threat level value exceeds the host alert value.
4. The method of claim 1, further comprising the steps of:
comparing the differential threat level value to a differential alert value; and
generating an alarm when the differential threat level value exceeds the differential
10 alert value.

5. A method for determining network security threat level, comprising the steps of:
receiving event data in response to an identified network event detected by a sensor; and
based upon the event data; determining a host threat level based upon a threat weighting assigned to the host associated with a threat weighting assigned to a host network block of which the host is a member.
6. The method of claim 5 wherein the host is a source device.
7. The method of claim 5 wherein the host is a destination device.
8. A method for determining network security threat level, comprising the steps of:
receiving event data in response to an identified network event detected by a sensor;
determining an event type based upon the event data; and
determining a source threat based upon a source threat weighting assigned to the source for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member.
9. A method for determining network security threat level, comprising the steps of:
receiving event data in response to an identified network event detected by a sensor;
determining an event type based upon the event data; and
determining a destination threat value based upon a destination threat weighting assigned to the destination for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member;
determining a destination vulnerability by associating the destination threat value with a destination vulnerability value based upon a vulnerability of a destination host for the event type.

10. A method for determining network security threat level, comprising the steps of:

- receiving event data in response to an identified network event detected by a sensor;
- 5 determining an event type based upon the event data; and
- determining a source threat based upon a source threat weighting assigned to a source for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member.
- determining a destination threat value based upon a destination threat weighting
- 10 assigned to the destination for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member;
- determining a destination vulnerability by associating the destination threat value with a destination vulnerability value based upon a vulnerability of a destination
- 15 host for the event type;
- determining an event validity based upon the source and the event type; and
- determining an event severity base upon the event type; and
- calculating the network security threat based upon the source threat, the destination vulnerability, the event validity, and the event severity.

20

11. A method for determining network security threat level, comprising the steps of:
- receiving event data in response to an identified network event detected by a sensor;
 - 5 determining an event type based upon the event data; and
 - determining a source threat based upon a source threat weighting assigned to a source for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member.
 - determining a destination threat value based upon a destination threat weighting
 - 10 assigned to the destination for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member;
 - determining a destination vulnerability by associating the destination threat value with a destination vulnerability value based upon a vulnerability of a destination
 - 15 host for the event type;
 - determining an event validity based upon the source and the event type; and
 - determining an event severity base upon the event type;
 - calculating an event threat based upon the source threat, the destination vulnerability, the event validity, and the event severity;
 - 20 calculating a compound host threat by associating a plurality of event threats over a time period with a number of correlated events in the time period.

12. A method for determining network security threat level, comprising the steps of:
- receiving event data in response to an identified network event detected by a sensor;
 - determining an event type based upon the event data; and
 - 5 determining a source threat based upon a source threat weighting assigned to a source for the event type associated with a network block threat weighting for the event type assigned to a host network block of which the host is a member.
 - determining a destination threat value based upon a destination threat weighting assigned to the destination for the event type associated with a network block threat
 - 10 weighting for the event type assigned to a host network block of which the host is a member;
 - determining a destination vulnerability by associating the destination threat value with a destination vulnerability value based upon a vulnerability of a destination host for the event type;
 - 15 determining an event validity based upon the source and the event type; and
 - determining an event severity base upon the event type;
 - determining an event threat based upon the source threat, the destination vulnerability, the event validity, and the event severity;
 - determining a first compound host threat value by associating a first plurality of
 - 20 event threats over a first time period with a first frequency number of correlated events in the first time period.
 - determining a second compound host threat value by associating a second plurality of event threats over a second time period greater than the first time period with a second frequency number of correlated events in the second time period; and
 - 25 determining a differential threat level by associating the first compound host threat value with the second host threat value.

13. A method for determining network security threat level, comprising the steps of:
receiving event data in response to an identified network event detected by a sensor;

determining an event type based upon the event data;

5 based upon the event data, perform the following steps:

determining a first host frequency threat level value by summing event threat level values for a host over a first time period dividing by the number of correlated events for the host in the first time period;

determining a second host frequency threat level value by summing event threat
10 level values for the host over a second time period greater than the first time period and associated with the number of correlated events for the host in the second time period;
and

determining a differential threat level numerator by multiplication of the first host frequency threat level value by the second time period;

15 determining a differential threat level denominator by multiplying the second host frequency value by the first time period, and

calculating a differential threat level by dividing the differential threat level numerator by the differential threat level denominator.

20